UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
WHITE PLAINS DIVISION

STEPHEN SCHLAUGIES, on behalf of himself and all others similarly situated, Plaintiff, v. BOSTON CHILDREN'S HEALTH PHYSICIANS, LLP d/b/a BOSTON CHILDREN'S HEALTH PHYSICIANS Defendant.	Case No. _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Stephen Schlaugies ("Plaintiff"), on behalf of himself and all others similarly situated, assert the following against Defendant Boston Children's Health Physicians, LLP d/b/a Boston Children's Health Physicians ("BCHP" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiff brings this class action complaint against Defendant for its (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information ("PII") and electronic private health information ("PHI"), including without limitation, Plaintiff's and Class Members' Social Security numbers, addresses, dates of birth, driver's license numbers, medical record numbers, health insurance information, billing information, and/or limited treatment information (collectively "PII/PHI"); (ii) failure to comply with laws, regulations, and industry standards to protect information systems that contain PII; (iii) unlawful disclosure of

Plaintiff's and Class Members' PII; and (iv) failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been disclosed.

2. Defendant is a medical provider that covers New York and Connecticut and specializes in comprehensive care for newborns, children, and adolescents. It boasts itself as the largest multi-specialty group in the New York and Connecticut area and has over 300 clinicians and 25 areas of medical expertise.

3. Defendant, on October 4, 2024, began mailing letters to individuals that described on September 6, 2024, Defendant's IT vendor informed them that it identified unusual activity in its systems. By September 10, 2024, Defendant had detected unauthorized activity in the their network, where a unauthorized third-party gained entry into Defendant's computer networks and systems, accessed the PII/PHI and exfiltrated the information from those systems.

4. Specifically, Defendant's disclosure stated that the company has experienced a "determined that an unauthorized third-party gained access to our network on September 10, 2024, and took certain files from our network" ("Cybersecurity Announcement").

5. Various news reports state that a popular ransomware gang, "BianLian" may be responsible for infiltrating Defendant's systems via its IT vendor and the gang now proclaims to have finance data, HR data, mailboxes and internal and external email correspondences, databases exports, PII/PHI and health records, health insurance records and children's and minor's data.

6. Defendant has yet to fully and accurately inform those affected of the extent of the Data Breach. It is not clear how many total victims Defendant thus far notified, however such information will be deduced through discovery.

7. The Data Breach occurred as a result of Defendant's failures, including lax security protocols. These failures enabled cybercriminals to gain access to Defendant's systems and/or

servers and exfiltrate the PII/PHI of potentially millions of individuals, including their names, Social Security numbers, addresses, dates of birth, driver's license numbers, medical record numbers, health insurance information, billing information, and/or limited treatment information. The exfiltrated PII/PHI remains in the hands of the cyber-criminals who seek to profit off the stolen PII/PHI by exploiting and stealing the identities of the Plaintiff and the Class Members.

8. The Data Breach was a direct and proximate result of Defendant's flawed systems configuration and design and Defendant's failure to implement and follow basic security procedures.

9. Because of Defendant's failures, unauthorized individuals were able to access and pilfer Plaintiff's and Class Members' PII. Plaintiff's and Class Members' identities are now at risk due to Defendant's negligent conduct because the highly valuable PII/PHI that Defendant collected and maintained has been accessed and acquired by data thieves.

10. As a result, the Plaintiff and Class Members are at substantially increased risk of future identity theft, both currently and for the indefinite future. Plaintiff's and Class Members' PII/PHI, including their Social Security numbers and driver's license numbers, that were compromised by cybercriminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft. Plaintiff and Class Members are at the peril of suffering financial risks, including but not limited to criminals opening new financial accounts in Plaintiff's and Class Member's names, using the stolen PII/PHI to obtain governmental benefits, and filing false tax returns.

11. Plaintiff, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory and injunctive relief. As set forth in more detail below, Plaintiff Schlaugies has suffered harm because

his personal and health information was compromised when Defendant's cyber security systems were breached.

12. Plaintiff seeks damage and injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members. Plaintiff also seeks to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that Plaintiff and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this Data Breach.

13. Given that information relating to the Data Breach, including the systems that were impacted and the configuration and design of Defendant's website and systems, remain exclusively in Defendant's control, Plaintiff anticipates additional support for their claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

14. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d)(2), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Members of the Class defined below, and a significant portion of putative Class Members are citizens of a different state than Defendant.

15. This Court has personal jurisdiction over Defendant because it is a New York domestic limited liability partnership with principal place of business is in this District. Defendant is also registered to do business in New York with the New York Department of State, Division of Corporations, and conducts substantial business in this District, and a substantial portion of the violations, acts, and omissions giving rise to this action occurred in this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District, Defendant does business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

A. Plaintiff

17. Plaintiff Stephen Schlaugies ("Plaintiff") is a citizen and resident of the State of New York. Plaintiff is a current and long standing patient of Defendant.

18. Plaintiff received a letter in the mail dated October 4, 2024, from the Defendant alerting him that his address, data of birth, medical record number, health insurance information, billing information, limited treatment information was compromised in the Data Breach.

B. Defendant

19. Defendant is a domestic New York limited liability partnership. Defendant is a medical service provider that provides comprehensive care for newborns, children, and adolescents across New York and Connecticut.

20. Defendant's registered address is 400 Columbus Avenue, Suite 200E, Valhalla, NY 10595. The multi-specialty healthcare group has more than 300 clinicians and its primary services include cardiology, oncology, pulmonology, and gastroenterology. Defendant provides services in over 55 practices and has over 500 employees. As part of its business, the Defendant collects valuable PII/PHI and sensitive health information from its patients or their guardians, such as Plaintiff and the Class Members.

BACKGROUND

I. Defendant Obtains, Collects, and Stores PII

21. Defendant is in complete operation, control, and supervision of its systems, and configured and designed its systems without adequate data security protections.

22. Defendant was entrusted with safely securing and safeguarding Plaintiff's and Class Members' PII/PHI.

23. Defendant did not properly verify, oversee, and supervise its entrustment of Plaintiff's and Class Members' PII/PHI. The information held by Defendant included unencrypted PII/PHI, a bulk of which was collected from Class Members as part of accessing Defendant's services that the submitted information would be kept safe, confidential and private.

24. The data collected and stored by health providers are among the most highly sensitive personally identifiable information. Health providers, in turn, bear the crucial responsibility to protect this data from compromise and theft. By obtaining, using, disclosing, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

25. Plaintiff and Class Members reasonably expect that a large and reputed health provider like the Defendant, who is entrusted with highly confidential information, will use the utmost care to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

26. Despite the sensitive nature of Defendant's business, Defendant failed to prioritize data and cybersecurity by adopting reasonable data and cybersecurity measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII/PHI. Defendant's system

security was so poor that a popular ransomware gang, "BianLian" was able to infiltrate Defendant's system and steal files containing the sensitive health information and PII.

27. Had Defendant followed industry guidelines and adopted reasonable security measures, Defendant would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiff's and Class Members' PII/PHI.

28. Defendant has an obligation to protect the PII/PHI belonging to Plaintiff and Class Members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII/PHI and medical records. Plaintiff and Class Members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

II. FTC Guidelines

29. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

30. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

31. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

32. The FTC further recommends that companies not maintain PII/PHI longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

33. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

34. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII/PHI, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Social Security information and other PII stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

35. Defendant was always fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII/PHI as well as collecting, storing, and using other confidential personal and financial information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

III. HIPAA Requirements and Violation

36. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

37. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

38. Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the PII/PHI belonging to Plaintiff and Class Members from unauthorized access and disclosure.

39. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

40. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

41. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.

IV. Industry Standards and Noncompliance

42. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII/PHI which they collect and maintain.

43. Some industry best practices that should be implemented by businesses dealing with sensitive PII/PHI, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

44. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

45. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

46. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

47. On or around September 10, 2024, Plaintiff's and Class Members' sensitive PII/PHI was compromised.

48. Through a post on its website on or around October 4, 2024, Defendant announced that "On September 6, 2024, our IT vendor informed us that it identified unusual activity in its systems. On September 10, 2024, we detected unauthorized activity on limited parts of the BCHP network" and the "unauthorized third-party gained access to our network on September 10, 2024, and took certain files from our network" including Plaintiff's and Class Members full names, Social Security numbers, phone numbers, mailing addresses, health insurance information, date of birth, billing information, sensitive medical information, driver's license number and other personal information (the "Data Breach").

49. Subsequently, news reports emerged that the ransomware gang, "BianLian" is responsible for infiltrating Defendant's system and BianLian added the stolen information from Defendant to its data leak site. According to the BianLian's site, the stolen data includes finance

data, HR data, mailboxes and internal and external email correspondences, database reports, PII and sensitive health data, children's and minor's data.

50. Despite the threat of data breaches and cyberattacks on the rise in the past several years, the Defendant failed to maintain proper security measures to protect the PII of the Plaintiff and Class Members.

51. Despite that the Data Breach occurred on or around September 10, 2024, the Defendant waited until at least October 4, 2024, to provide *any* notice to the affected individuals, according to the Cybersecurity Announcement published on its website. On October 4, 2024, when Defendant began notifying affected individuals, its notice stated:

What Happened?

> On September 6, 2024, our IT vendor informed us that it identified unusual activity in its systems. On September 10, 2024, we detected unauthorized activity on limited parts of the BCHP network and immediately initiated our incident response protocols, including shutting down our systems as a protective measure. We also began an investigation with a third-party forensic firm and determined that an unauthorized third-party gained access to our network on September 10, 2024, and took certain files from our network.

52. Defendant admitted that an unauthorized third-party bad actor accessed its network systems containing the sensitive PII/PHI. The stolen information in the Data Breach included, without limitation, names, Social Security numbers, addresses, dates of birth, driver's license numbers, medical record numbers, health insurance information, billing information, and/or limited treatment information. Other public reporting of the Data Breach is much larger in scope than what Defendant has disclosed.

53. "BianLian" claims to have finance and HR data, email correspondence, database dumps, personally identifiable and health records, health insurance records, and data related to children.

54. Plaintiff's PII/PHI was disclosed without his authorization to unknown third parties as a result of the Data Breach.

55. As a result of the Data Breach, the Plaintiff spent time and effort researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, reviewing credit monitoring services, and dealing with phishing attempts via email and telephone calls using the information taken in the Data Breach.

56. After receiving the notice letter from the Defendant, Plaintiff spent time researching the Data Breach to confirm that his PII/PHI had been compromised in the Data Breach.

57. The Data Breach has caused the Plaintiff to suffer from severe anxiety and stress from concerns that they face an increased risk of financial fraud, identity theft, tax fraud, medical fraud and other types of monetary harm as a result of the stolen information. Plaintiff places significant value in the security of his PII/PHI and the confidentiality of the health information entrusted to the Defendant.

58. Plaintiff and Class Members suffered actual damages as a result of the failures of Defendant to adequately protect the sensitive information entrusted to it, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, tax and medical fraud, the loss in value of their PII, the loss of confidentiality of the health information and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

59. As a result of the Data Breach, Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature

of the PII/PHI compromised by the Data Breach. As mentioned above, they also continue to suffer from anxiety and fear of financial fraud and identity theft.

II. Defendant's Data Security Failures Caused the Data Breach

60. Up to, and including, the period when the Data Breach occurred, Defendant breached its duties, obligations, and promises to Plaintiff and Class Members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers were susceptible to a data breach;

d. Properly oversee its IT vendors;

e. implement certain protocols that would have prevented unauthorized programs, such as ransomware and malware, from being installed on its systems that accessed individual's personal information and otherwise would have protected their sensitive personal information;

f. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented individual's sensitive PII/PHI from being stolen. Specifically, there are recommended, available measures to prevent data from

leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

g. adequately safeguard individual's sensitive PII/PHI and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

III. Defendant's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

61. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

63. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

64. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations. These include recent cases concerning health-

related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.

65. Prior to the Data Breach, and during the breach itself, Defendant failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security.

66. Furthermore, by failing to have reasonable data security measures in place, Defendant engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

IV. The Value of the Disclosed PII/PHI and Effects of Unauthorized Disclosure

67. Defendant understood the protected PII/PHI it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII/PHI and those who would use it for wrongful purposes.

68. PII/PHI is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers.

69. Sensitive personal information commonly stolen in data breaches has economic value. The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

70. By accessing an individual's personal information, the bad actors can cause upheaval in the individual's life. They could withdraw funds from the bank accounts, get new credit cards or loans, lock the individual out of their own bank accounts or social media accounts, file false tax returns and destroy their credit score. Stolen Social Security numbers also make it

possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

71. The forms of PII/PHI involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security and driver's numbers and treatment information cannot be easily replaced. Even when such numbers and information are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

72. The Social Security Administration (''SSA") warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with

> your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

73. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII/PHI to steal and then sell.

74. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII/PHI secure are long lasting and severe.

75. To avoid detection, identity thieves often hold stolen data for months or years before using it. The stolen PII/PHI is freely available on the dark web and thus, Plaintiff and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

76. Thus, Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

77. As a highly sophisticated entity that handles sensitive PII/PHI, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' PII/PHI to protect against anticipated threats of intrusion of such information.

78. Identity thieves use stolen PII/PHI for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

79. The PII/PHI exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

80. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used.

81. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

82. PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

83. Plaintiff and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

84. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

V. The Data Breach Damaged Plaintiff and the Class Members

85. According to research, sensitive PII can sell for as much as $363 per record.[1] As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII/PHI is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

86. As a result of Defendant's deficient security measures, Plaintiff and Class Members are also under a constant threat of their PII/PHI being used by criminals for identify theft and other fraud-related crimes.

87. Plaintiff and Class Members face a substantial and imminent risk of fraud and identity theft as their names and other PII/PHI have now been linked. These specific types of information are associated with a high risk of fraud.

88. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

89. Plaintiff and Class Members also suffered a "loss of value" of their sensitive PII/PHI when it was stolen by hackers in the Data Breach. A robust market exists for stolen PII/PHI. Hackers sell PII on the dark web—an underground market for illicit activity, including

[1] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

the purchase of hacked PII—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiff and Class Members. Here, the stolen information already appears on the data leak site of ransomware gang, "BianLian."

90. Identity thieves can also combine data stolen in the Data Breach with other information about the Plaintiff and Class Members gathered from underground sources, public sources, or even Plaintiff's and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiff's and Class Members' names, taking out loans in Plaintiff's and Class Members' names, using Plaintiff's and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiff's and Class Members' information, obtaining Social Security numbers in Plaintiff's and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

91. Plaintiff and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud and the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Defendant has disclosed little information about the Data Breach, forcing customers to continue to monitor their accounts indefinitely.

92. Plaintiff and Class Members who experience identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that

bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

93. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again, especially when that individual spent significant time monitoring their accounts and rectifying any problems that arose.

94. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including Social Security number) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

95. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. The stolen PII/PHI is freely available on the dark web which may be used at any time by the bad actors, including after many months or more to target Plaintiff and the Class Members. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

VI. Defendant's Failure to Timely Notify Plaintiff and Class Members

96. As detailed above, the Data Breach occurred on or around September 10, 2024. Defendant claims to have discovered the Data Breach on or around September 10, 2024, and only began notifying the Plaintiff and Class Members of the Data Breach on or around October 4, 2024.

97. Defendant's failure to realize that its systems had been compromised resulted in a squandering of time. This is time that could have been used by Plaintiff and Class Members to take steps to mitigate the damage caused by the Data Breach.

98. Instead, Defendant concealed the Data Breach for more than three weeks and potentially even longer, allowing the unauthorized third-party to potentially exploit Plaintiff's and Class Members' PII without any mitigation steps being taken.

99. Plaintiff and Class Members were deprived of the opportunity to take any steps to prevent damage by Defendant's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

100. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose PII was compromised in the Data Breach made public by Boston Children's Health Physicians in October 2024 (the "Nationwide Class").

101. Excluded from the Class are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

102. Plaintiff reserves the right to modify, expand or amend the above Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

103. Certification of Plaintiff's claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

104. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Class are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. There are likely tens of thousands of Members of the Class. Although, the precise number of Class Members is unknown to Plaintiff.

105. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

106. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendant engaged in active misfeasance and misconduct alleged herein;

b. Whether Defendant owed a duty to Class Members to safeguard their sensitive PII;

c. Whether Defendant breached its duty to Class Members to safeguard their sensitive PII;

d. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

e. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Defendant's failure to provide adequate security proximately caused Plaintiff's and Class Members' injuries; and

g. Whether Plaintiff and Class Members are entitled to declaratory and injunctive relief.

107. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of all Class Members because Plaintiff, like other Class Members, suffered theft of their sensitive personal information in the Data Breach.

108. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because he is a Member of the Class and his interests do not conflict with the interests of other Class Members that they seek to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the Class's interests.

109. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by the Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

110. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Class such that final declaratory or injunctive relief is appropriate.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of the Plaintiff and the Nationwide Class)

111. Plaintiff re-alleges and incorporates by reference all of the allegations contained above as if fully set forth herein.

112. Defendant obtained Plaintiff's and Class Members' PII/PHI. Upon information and belief, Defendant collects the highly sensitive PII in course of its business of providing healthcare related services to newborns, children and adolescents.

113. By collecting and storing sensitive PII/PHI, Defendant had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Defendant's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

114. Defendant owed a duty of care to the Plaintiff and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

115. Defendant was subject to an "independent duty" untethered to any contract between the Plaintiff and Class Members and Defendant.

116. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' valuable and sensitive PII.

117. Defendant's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against malware;

b. failure to comply with industry standards for software and server security;

c. failure to track and monitor access to its network;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to remove, delete, or destroy highly sensitive personal information of individuals that is no longer being used for any valid business purpose;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing PII from its network while the Data Breach was taking place; and

i. failure to oversee the entrustment of PII.

118. It was foreseeable to Defendant that a failure to use reasonable measures to protect its customers' sensitive PII could result in injury to its clients, Plaintiff and the Class Members. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendant given the known frequency of data breaches and various warnings from industry experts. The reported hackers who infiltrated Defendant's systems have been known to be associated with other health care related breaches, including Murfreesboro Medical Clinic April 2023, Affiliated Dermatologists & Dermatologic Surgeons P.A. in March 2024, and Texas Retina Associates (hit in April 2024.

119. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as alleged herein. Plaintiff and Class Members are entitled to damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

120. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of the Plaintiff and the Nationwide Class)

Negligence Per Se Under the FTC Act

121. Plaintiff re-alleges and incorporates by reference all of the allegations contained above as if fully set forth herein.

122. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect sensitive PII.

123. Various FTC publications and orders also form the basis of Defendant's duty.

124. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

125. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

126. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as alleged herein. Plaintiff and Class Members are entitled to damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

128. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. Plaintiff's and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

Negligence Per Se Under HIPAA

130. HIPAA imposes a duty on Defendant to implement reasonable safeguards to protect Plaintiff's and Class members' PII/PHI. 42 U.S.C. § 1302(d), *et seq*.

131. HIPAA also requires Defendant to render unusable, unreadable, or indecipherable all PII/PHI it collected. Defendant was required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

132. Defendant violated HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' PII/PHI.

133. Defendant violated HIPAA by failing to properly encrypt the PII/PHI it collected.

134. Defendant's failure to comply with HIPAA constitutes negligence *per se*.

135. Plaintiff and Class members are within the class of persons that HIPAA is intended to protect.

136. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' PII/PHI in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

137. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as alleged herein. Plaintiff and Class Members are entitled to damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

138. Defendant's violation of HIPAA constitutes negligence *per se*.

139. Plaintiff's and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of the Plaintiff and the Nationwide Class)

140. Plaintiff re-alleges and incorporates by reference all of the allegations contained above as if fully set forth herein.

141. Defendant entered into contracts, including with Plaintiff to provide healthcare related services to Plaintiff. The contract was a pre-requisite before Defendant could provide its services.

142. By providing their PII/PHI, and upon Defendant's acceptance of this information, Plaintiff and the Class, on one hand, and Defendant, on the other hand, entered into contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

143. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach. These contracts were made expressly for the benefit of the Plaintiff and the Class, as Plaintiff and Class Members were the intended beneficiaries of the contracts entered into between Defendant and its patients. Defendant knew that, if it were to breach these contracts with patients, then its patients data, like that of the Plaintiff's and Class Members—would be harmed.

144. The implied contracts between Defendant and Plaintiff and Class Members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class Members' PII/PHI. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above.

145. Upon information and belief, Plaintiff and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts between Defendant and patients that upon information and belief, include obligations to protect, safeguard, and keep secure the PII/PHI of the Plaintiff and Class Members.

146. Defendant's representations required Defendant to implement the necessary security measures to safeguard the PII/PHI of Plaintiff and Class Members and not take unjustified risks when storing the PII.

147. Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

148. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII/PHI belonging to Plaintiff and Class Members, and allowing unauthorized persons to access Plaintiff's and Class Members' PII/PHI,

149. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of PII/PHI, and are entitled to damages in an amount to be proven at trial.

150. Plaintiff and Class Members were harmed by Defendant's conduct as a direct and proximate result of Defendant's breach of its contracts with its clients and are entitled to the damages they have sustained. Plaintiff and Class Members are entitled to damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

151. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of the Plaintiff and the Nationwide Class)

152. Plaintiff re-alleges and incorporates by reference all of the allegations contained above as if fully set forth herein.

153. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of PII, and also paid monies to Defendant to avail Defendant's healthcare related services.

154. Defendant accepted or knew that Plaintiff and Class Members conferred a monetary benefit to Defendant, and accepted and retained those benefits by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's and Class Members' retained data and used Plaintiff's and Class Members' PII for business purposes.

155. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for and oversee adequate data privacy infrastructure, practices, and procedures.

156. In equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff's and Class Members because Defendant failed to oversee, implement, or adequately implement, the data privacy and security practices and procedures that Plaintiff and the Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

157. As a result of Defendant's conduct, Plaintiff's and Class Members have been injured as alleged herein.

158. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

159. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pled.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of the Plaintiff and the Nationwide Class)

160. Plaintiff re-alleges and incorporates by reference all of the allegations contained above as if fully set forth herein.

161. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

162. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and statutory duties to reasonably safeguard Plaintiff's and Class Members' sensitive PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches. Plaintiff alleges that Defendant's data security practices remain inadequate.

163. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their sensitive PII/PHI and remain at imminent risk that further compromises of their PII will occur in the future.

164. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure Plaintiff's and Class Members' sensitive PII/PHI, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure Plaintiff's and Class Members' sensitive PII.

165. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive PII/PHI.

166. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have

an adequate remedy at law, because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

167. The hardship to the Plaintiff and Class Members if an injunction does not issue greatly exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, Plaintiff and the Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

168. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose confidential information would be further compromised.

REQUEST FOR RELIEF

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendant including the following:

A. Determining that this matter may proceed as a class action and certifying the Class asserted herein;

B. Appointing the Plaintiff as representatives of the applicable Class and and/or subclass and appointing Plaintiff's counsel as Class Counsel;

C. An award to Plaintiff and the Classes of damages, including actual, compensatory, punitive, and nominal damages as set forth above;

D. Disgorgement into a common fund for the benefit of the Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant as a result of the conduct and Data Breach as set forth above;

E. Ordering injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; and (iv) timely notify individuals of any future data breaches;

F. Entering a declaratory judgment stating that Defendant owes a legal duty to secure Plaintiff's and Class Members' sensitive PII, to timely notify its clients and any person or business entity of any data breach, and to establish and implement data security measures that are adequate to secure sensitive personal information;

G. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

H. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

I. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: October 18, 2024

Respectfully submitted,

/s/ Christian Levis
Christian Levis
Peter Demato
Radhika Gupta
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500

clevis@lowey.com
pdemato@lowey.com
rgupta@lowey.com

Anthony M. Christina (pro hac vice forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
achristina@lowey.com

Counsel for Plaintiff Stephen Schlaugies and the Proposed Class